PCT/DE03/03853

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 59 270.5

Anmeldetag: 17. Dezember 2002

Anmelder/Inhaber: Wincor Nixdorf International GmbH, Paderborn/DE

Bezeichnung: Personalisierung von Sicherheitsmoduln

IPC: H 04 L 9/32

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 16. Dezember 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Agurks

A 9161
06/00
EDV-L

Personalisierung von Sicherheitsmoduln

Die Erfindung betrifft die Personalisierung von kryptographischen Sicherheitsmoduln.

Stand der Technik

Für den Betrieb insbesondere von Geldautomaten werden Sicherheitsmodule verwendet, die einen kryptographischen Prozessor und einen Schlüsselspeicher umfassen. Bei dem Betrieb des Geldautomaten werden durch den Sicherheitsmodul alle Nachrichten von oder zu einem Zentralsystem durch den Sicherheitsmodul kryptographisch gesichert. Der Schlüsselspeicher ist von außen nicht auslesbar, sondern kann nur für kryptographische Operationen verwendet werden, so dass ein einmal in den Sicherheitsmodul übertragener Schlüssel nicht mehr kompromittiert werden kann.

Dieser als Personalisierung bezeichnete Vorgang ist sicherheitstechnisch kritisch. Dies gilt in besonderem Maße für die bislang verwendete symmetrische Verschlüsslung, z.B. das DES-Verfahren, bei dem ein und derselbe Schlüssel zur Ver- wie auch Entschlüsslung verwendet wird. Daher ist beim Hersteller des Sicherheitsmoduls ein hoher Aufwand notwendig, um die verwendeten Schlüssel gegen Ausspähung zu sichern. Insbesondere muss die Personalisierung in zugangsgesicherten Räumlichkeiten mit speziellem Personal erfolgen. Bei Verwendung nur weniger Masterschlüssel ist ein besonders hoher Sicherheitsaufwand notwendig. Eine kundenspezifische Programmierung erfordert einen großen Logistik- und Lageraufwand, einschließlich der Bewachung von Lager und Transport.

Es ist Aufgabe der Erfindung ein Verfahren bereit zu stellen, durch welches die Personalisierung unmittelbar während der Inbetriebnahme durch den Kunden selbst am Einsatzort oder einer anderen nicht besonders gesicherten Umgebung erfolgen kann.

In der Patentschrift US 6,442,690 B1 wird ein Personalisierungssystem für einen kryptographischen Modul beschrieben. Hierbei wird der kryptographische Modul mit einem vorläufigen Schlüssel versehen. Zur Personalisierung wird zunächst überprüft, ob dieser vorläufige Schlüssel vorhanden ist, und gegebenenfalls gegen einen neuen ausgetauscht. Die neuen Schlüssel werden dabei über ein Schlüsselmanagement von dem Personalisierer bereitgestellt. Vorgeschlagen wird auch die Verwendung von asymmetrischen Verfahren, bei denen ein Schlüsselpaar aus öffentlichem Schlüssel und geheimem Schlüssel Verwendung findet. Die Eigenschaften und Vorteile von asymmetrischen Verfahren gegenüber symmetrischen Verfahren sind aus der einschlägigen Literatur bekannt; ihre Kenntnis wird im folgenden ohne weiteres vorausgesetzt.

In der Patentschrift US 6,298,336 B1 wird ein transportables Aktivierungsgerät für Chipkarten mit Bezahlfunktion beschrieben, wobei die Chipkarten bis zur, kryptographisch gesicherten, Aktivierung für die vorgesehenen Anwendungen unbenutzbar sind.

In der Patentschrift DE 199 19 909 C2 wird ein Verfahren beschrieben, bei dem eine Nachricht mit symmetrischer Verschlüsslung signiert und im Klartext übertragen werden kann, ohne dass die die Signatur bildende Stelle über den geheimen Schlüssel verfügen muss. Dieses Verfahren wird optional in einer Ausführungsform der Erfindung eingesetzt.

Die Erfindung verwendet die Erkenntnis, dass ein transportables Personalisiergerät, das ähnlich wie ein Sicherheitsmodul aufgebaut ist und insbesondere einen geschützten Schlüsselspeicher und einen damit operierenden kryptographischen Prozessor enthält, eine besonders vorteilhafte Handhabung der durch die Erfindung beschriebenen Methode

erlaubt. Hier ist insbesondere die Verwendung von Chipkarten von großem Vorteil, da diese zusammen mit mobilen Computern ein portables Personalisiergerät leicht verfügbar machen. Wird ein solches Personalisiergerät vor Ort mit dem Sicherheitsmodul verbunden, ist bereits hierdurch ein hohes Maß an Sicherheit dafür gegeben, dass auch das richtige Sicherheitsmodul personalisiert wird. Ein besonderer Vorteil besteht darin, dass das Sicherheitsmodul sich bereits am endgültigen Ort befindet und daher keine weiterer Transport erforderlich ist, der durch Bewachung zu sichern wäre. In der bevorzugten Ausführungsform wird zusätzlich eine gegenseitige Authentisierung von Sicherheitsmodul und Personalisierer vorgesehen, bei der der Sicherheitsmodul vom Hersteller vorläufig initialisiert, aber nicht personalisiert wird. Diese Initialisierung kann, bis gegebenenfalls auf laufende Seriennummern, bei allen Moduln gleich sein.

Es handelt sich um einen Sicherheitsmodul, einen Personalisierer und eine Methode zu deren Benutzung, wobei der Sicherheitsmodul den geheimen Schlüssel eines Schlüsselpaares für asymmetrische Verschlüsselung enthält, der Personalisierer ein Zertifikat über den öffentliche Schlüssel des Schlüsselpaares erzeugt und zusammen mit dem öffentlichen Schlüssel eines Zentralsystems an den Sicherheitsmodul sendet. Der Sicherheitsmodul verwendet dieses Zertifikat und den öffentlichen Schlüssel zur Sicherung der Kommunikation mit einem Zentralsystem, insbesondere im Bankenbereich.

Beschreibung

In Fig. 1 wird die Erfindung schematisch im Zusammenhang gezeigt. Ein Bankautomat 10 enthält einen Sicherheitsmodul 12 und ist über eine Netzwerkverbindung 24 eines Netzwerks 20 mit einem Zentralsystem 22 im späteren Einsatz

verbunden. Ferner ist ein Personalisierer 30 gezeigt, der über eine Chipkarte 32 mit kryptographischem Prozessor und gesichertem Schlüsselspeicher verfügt. Die gestrichelte Linie in Fig. 1 soll andeuten, dass der Personalisierer 30 nur vorübergehend in die räumliche Nähe des Sicherheitsmoduls 10 gebracht und über die Datenverbindung 34 verbunden ist.

Die Bezeichnung "Zentralsystem" wird generisch für im Betriebszustand mit dem Sicherheitsmodul verbundenen Kommunikationsgegenstellen verwendet.

Der Personalisierer ist bevorzugt ein mobiler Computer, der mit einer Chipkarte als kryptographischer Einheit ausgestattet ist. Diese Chipkarte umfasst einen gesicherten Schlüsselspeicher und führt mit den dort gespeicherten Schlüsseln die benötigten kryptographischen Verfahren über Daten aus, die via Schnittstelle der Chipkarte übertragen werden. Der Schlüsselspeicher ist insofern gesichert, dass das Protokoll auf der Schnittstelle vollständig von dem Prozessor auf der Chipkarte überwacht wird und so gestaltet ist, dass die geheimen Schlüssel aus dem Schlüsselspeicher nicht über die Schnittstelle übertragen werden; lediglich ihre Anwendung auf Daten ist möglich. Entsprechend wird die Integrität öffentlicher Schlüssel entweder durch Speicherung im Schlüsselspeicher oder Ablage von kryptographischen Hashwerten im Schlüsselspeicher bewirkt. Wenngleich die bekannte Ausführungsform als Chipkarte nach ISO bevorzugt ist, kann auch eine Prozessorkarte im PCMCIA-Format oder ein externer per USB oder Firewire angeschlossener Modul verwendet werden. Ohne weiteres kann auch die gesamte Software und der Schlüsselspeicher in dem mobilen Computer selbst enthalten sein, wenngleich dies wegen der geringeren Sicherheit bei derzeitig verfügbaren mobilen Computern nicht die bevorzugte Ausführung ist.

Zusätzlich zu der kryptographischen Verarbeitungsmöglichkeit und dem sicheren Schlüsselspeicher verfügt der Personalisierer über eine Kommunikationsschnittstelle, mit der vorübergehend eine Verbindung zum Sicherheitsmodul hergestellt werden kann. Im einfachsten Fall ist dies eine serielle Verbindung nach V.24, wobei ein Kabel mit Steckern vorübergehend eingesteckt wird und die Verbindung so durch einen Benutzer gesteuert wird. Andere Datenverbindungen wie I^2C, USB, Firewire usw. sind gleichfalls möglich. Drahtlose Verbindungen über Infrarot oder Funk, wie IrDA oder Bluetooth sind gleichermaßen gut verwendbar; hier entfällt die physische Herstellung einer Verbindung. Bluetooth hat den zusätzlichen Vorteil, dass eine Verschlüsselung der Kommunikation eingebaut ist, wenngleich das Schlüsselmanagement der Anwendung überlassen bleibt. Dies ist hier ohnehin der Fall.

Kabel- und Infrarotverbindungen haben den Vorteil, dass von der Bedienperson recht gut sichergestellt werden kann, dass das beabsichtigte Gerät personalisiert wird, wenn die Verbindung unmittelbar zu dem zu personalisierenden Sicherheitsmodul führt. Für manche Einsatzzwecke mag diese Authentisierung ausreichend sein, so dass die im folgenden beschriebene bevorzugte kryptographische Authentisierung entfallen kann.

Der Sicherheitsmodul befindet sich nach der Auslieferung und vor Beginn der Personalisierung in einem Personalisierungszustand, der von dem nachfolgenden Betriebszustand abweicht.

Die Verbindung zwischen Personalisierer und Sicherheitsmodul ist bevorzugt eine kryptographisch gesicherte Verbindung nach bekannten Verfahren, wie sie beispielsweise als TLS im Zusammenhang mit HTTPS bekannt sind. Ist die Verbindung aufgebaut und verfügbar, dann

stellen diese Verfahren sicher, dass die nachfolgende Kommunikation weder abgehört noch modifiziert werden kann. In der Regel wird hierzu ein zufälliger Schlüssel verwendet, der entweder nach dem Diffie-Hellmann-Verfahren ohne Authentisierung oder im Rahmen einer Authentisierung, so z.B. gemäß der Veröffentlichung WO 91/14980, bereitgestellt wird. Die Sicherheitsanforderungen an die gegenseitige Authentisierung, die je nach Einsatzfall zu ermitteln sind, bestimmen damit die Anforderungen an die zu verwendende Authentisierung. Hierzu kann auch die genannte Patentschrift DE 199 19 909 C2 dienen, nach der der Hersteller ein Zertifikat in einen Sicherheitsmodul einbringen kann, ohne über den Schlüssel für die Verifizierung zu verfügen. Auch ist es möglich, beim Hersteller jeden Sicherheitsmodul mit einem zufälligen Schlüssel auszustatten, der in den Begleitpapieren enthalten ist oder unabhängig über sichere Wege übermittelt wird. Die gegenseitige Authentisierung erfolgt dann über bekannte Challenge-Response-Verfahren, z.B. gemäß dem europäischen Patent EP 552392.

Ist die gesicherte Verbindung zwischen Sicherheitsmodul und Personalisierer aufgebaut, dann sendet der Sicherheitsmodul darüber den öffentlichen Schlüssel eines Schlüsselpaares, dessen privater Schlüssel in seinem gesicherten Schlüsselspeicher abgelegt ist. Dieses Schlüsselpaar, im folgenden auch als Modulschlüssel bezeichnet, kann bereits bei der Herstellung generiert werden, da der private Schlüssel den Sicherheitsmodul nicht verlassen und daher beim Hersteller auch nicht kompromittiert werden kann.

Bevorzugt wird das Schlüsselpaar jedoch erst im Rahmen der Personalisierung erzeugt, weil dann der Einfluss des Herstellers geringer ist und damit seine Sicherheitsvorkehrungen weniger aufwendig sind. Außerdem kann ein vom Personalisierer vorgegebener Modifikator, in der Literatur auch als 'salt' bezeichnet, mit übertragen werden, der das erzeugte Schlüsselpaar beeinflusst.

Nunmehr überträgt der Sicherheitsmodul den öffentlichen Schlüssel an den Personalisierer. Dieser verwendet den bei sich gespeicherten geheimen Schlüssel eines weiteren, im folgenden als Signierschlüssel bezeichneten Schlüsselpaars, und signiert damit den von dem Sicherheitsmodul erhaltenen öffentlichen Modulschlüssel. Eine solche Signatur eines öffentlichen Schlüssels, mit oder ohne diesen signierten öffentlichen Schlüssel, wird im folgenden als Zertifikat bezeichnet.

Der Personalisierer sendet das Zertifikat über die bestehende gesicherte Verbindung zurück an den Sicherheitsmodul, welcher das Zertifikat dauerhaft und sicher gegen Veränderung für die Verwendung im nachfolgend beschriebenen Betriebszustand speichert. Dabei wird, wie oben erwähnt, die Integrität mittels des sicheren Schlüsselspeichers gesichert.

In einer Weiterbildung der Erfindung sendet der Personalisierer zusammen mit dem Zertifikat auch einen öffentlichen Schlüssel eines Zentralsystems zurück, mit dem der Sicherheitsmodul zukünftig im Betriebszustand verbunden werden soll. Bevorzugt wird dieser öffentliche Schlüssel gleichfalls von dem Personalisierer mit einem Zertifikat versehen, obwohl der Sicherheitsmodul dieses nicht prüfen kann, bis im Sicherheitsmodul ein gesicherter öffentlicher Schlüssel des Personalisierers vorliegt. Dieser sendet daher als drittes seinen öffentlichen Schlüssel zusammen mit einem weiteren Zertifikat. Dieses kann entweder vom Zentralsystem ausgestellt sein und kann dann mit dem gleichfalls übertragenen öffentlichen Schlüssels des Zentralsystems geprüft werden. Diese Zirkularzertifizierung ist eher als Plausibilitätsprüfung anzusehen, weil der Personalisierer ohne weiteres ein beliebiges Schlüsselpaar für das Zentralsystem selbst erzeugen und sodann die notwendigen Zertifikate herstellen kann.

Besser ist die Lösung, bei der der öffentliche Schlüssel des Personalisierers durch ein weiteres Schlüsselpaar des

Herstellers signiert wurde, wobei der Hersteller seinen öffentlichen Schlüssel bei der Herstellung in den Sicherheitsmodul eingetragen hat. Das entsprechende Zertifikat wird vom Personalisierer an den Sicherheitsmodul übertragen.

Damit ist dann beim Aufbau der Verbindung eine Authentisierung des Personalisierers gegenüber dem Sicherheitsmodul nicht mehr notwendig, da im Rahmen der Personalisierung die vom Personalisierer übertragenen Zertifikate geprüft werden. Dass dann der öffentliche Modulschlüssel eventuell unberechtigt ausgelesen werden kann, ist nach dem Prinzip der asymmetrischen Verschlüsslung unkritisch. Lediglich sind vom Hersteller die Signierschlüssel der Kunden nach Bedarf zu signieren und der eigene öffentliche Schlüssel in den Sicherheitsmodul einzutragen.

Wenn durch die Signierung des Signierschlüssels des Personalisierers ohnehin ein Datenaustausch zwischen Hersteller und Betreiber des Personalisierers stattfindet, wird bevorzugt auch der öffentliche Schlüssel des Herstellers mit ausgetauscht. Der Sicherheitsmodul erzeugt dann zum Abschluss des Herstellungsvorgangs ein weiteres Schlüsselpaar, das permanent erhalten bleibt und zur sicheren Identifizierung des Sicherheitsmoduls dient. Der zugehörige öffentliche Schlüssel wird beim Hersteller signiert und das Zertifikat in den Sicherheitsmodul geladen. Damit kann der Sicherheitsmodul durch Signierung seiner Seriennummer und anderer vom Personalisierer vorgegebener Daten wie Zeitstempel und Zufallszahlen, seine Identität beweisen, sich also authentisieren.

Nunmehr wird die Verbindung zwischen Personalisierer und Sicherheitsmodul abgebaut und so der Personalisierer vom Sicherheitsmodul getrennt. Das Sicherheitsmodul wechselt damit in den normalen Betriebszustand, in dem eine weitere

Personalisierung nicht möglich ist. Eine erneute Personalisierung kann über einen direkten Eingriff im Sicherheitsmodul (oder auch einen wie auch immer gegen Missbrauch gesicherten Befehl, beispielsweise vom Zentralsystem) erzwungen werden. Dieses Rücksetzen in den Personalisierungszustand ist jedoch damit verbunden, dass der Sicherheitsmodul das Schlüsselpaar löscht und im Rahmen der nachfolgenden Personalisierung die Generierung eines neuen Schlüsselpaares erzwingt.

In dem auf die Personalisierung folgenden Betriebszustand wird nunmehr eine Verbindung zwischen Sicherheitsmodul und Zentralsystem hergestellt, die gleichfalls durch kryptographische Mittel, insbesondere Sitzungsschlüssel, gesichert wird. Hierbei sendet der Sicherheitsmodul das vom Personalisierer ausgestellte Zertifikat zusammen mit seinem öffentlichen Schlüssel an das Zentralsystem. Dem Zentralsystem wurde zuvor der öffentliche Schlüssel des Personalisierers durch eine integritätskontrollierte Verbindung übermittelt. (Beispielsweise wird die Chipkarte vom Zentralsystem personalisiert). Das Zentralsystem kann damit überprüfen, ob der Sicherheitsmodul für die nachfolgenden Transaktionen berechtigt ist und beispielsweise zuverlässig übermitteln kann, dass für eine Auszahlung eines mitgesendeten Betrages eine authentische Bankkarte für eine bestimmte Kontonummer vorliegt. Indem der Sicherheitsmodul von dem Personalisierer den öffentlichen Schlüssel des Zentralsystems erhalten hat, ist wiederum für den Sicherheitsmodul sichergestellt, dass die vom Zentralsystem erhaltenen Nachrichten, z.B. der Auftrag für die Auszahlung eines Geldbetrags, von einem berechtigten Zentralsystem stammen.

Aus Gründen der Kompatibilität oder der Geschwindigkeit kann auch ein symmetrischer Schlüssel von dem Zentralsystem in das Sicherheitsmodul übertragen werden, der dann in den sicheren Schlüsselspeicher eingetragen wird und für eine beschränkte Zeit für Transaktionen nach bisherigen auf

symmetrischer Kryptographie beruhenden Verfahren benutzt wird.

In der bevorzugten Ausführungsform wird jede Personalisierung auf der Chipkarte in einem Protokoll aufgeführt. Damit ist sichergestellt, dass die ausgegebenen Zertifikate jederzeit nachvollzogen werden können. Bei einer Kompromittierung der Chipkarte steht durch Sperrung des zugehörigen öffentlichen Schlüssels im Zentralsystem schnell eine wirksame Gegenmaßnahme zur Verfügung.

Ein nicht durch die Erfindung personalisierter Sicherheitsmodul muss weder bei der Lagerung noch beim Transport besonders bewacht werden, da er ohne Personalisierung nicht verwendbar ist. Damit liegt auch der Wert des Moduls nicht wesentlich über dem Herstellungswert und ist zudem nicht kundenspezifisch.

Da der Personalisierer in der bevorzugten Ausführungsform nur mit einer Chipkarte als Kryptographieeinheit verwendbar ist, ist, bei entsprechender Gestaltung der Software, lediglich die Chipkarte gegen Missbrauch zu sichern. Hierfür haben insbesondere Banken unter Verwendung des Vier-Augen-Prinzips wirksame administrative Verfahren zur Verfügung.

Eine Variante der Erfindung verwendet das vorhandene, im Betriebszustand ohnehin benötigte Datennetzwerk zur Verbindung des Sicherheitsmoduls mit dem Personalisierer. Dies erlaubt es, dass der Personalisierer gesichert betrieben wird und auch in das Zentralsystem integriert werden kann. In letzterem Fall vereinfacht sich die gegen Verfälschung zu sichernde Übertragung des öffentlichen Signierschlüssels vom Signier- zum Zentralsystem.

In diesem Fall wird über entsprechende Protokollelemente eine kryptographisch insbesondere gegen Verfälschung gesicherte Verbindung aufgebaut. Als Teil der sicheren

Identifizierung und Authentisierung ist sicherzustellen, dass auch der "richtige" Sicherheitsmodul personalisiert wird.

Eine erste Lösung besteht darin, dass eine Bedienperson über eine temporäre direkte Datenverbindung eine Einmal-Transaktionsnummer eingibt, die an den Personalisierer gesendet wird. Diese Transaktionsnummer kann in Sicherheitsumschlägen transportiert werden und beispielsweise 16 oder mehr Zeichen umfassen. Die Verbindung zum Sicherheitsmodul braucht auch nicht gesichert zu sein, da die Transaktionsnummer unmittelbar nach der Eingabe wertlos wird. Es genügt also eine einfache Tastatur mit einer einfachen seriellen Schnittstelle, die temporär mit dem Sicherheitsmodul verbunden wird. Hat der Sicherheitsmodul ohnehin eine Tastatur, beispielsweise für Diagnosezwecke, dann kann diese für die Eingabe der Transaktionsnummer verwendet werden.

Für sehr lange Transaktionsnummern wird ein mobiler Computer mit einer der oben angegebenen Schnittstellen verwendet. Bevorzugt werden dann die Transaktionsnummern auf einer Chipkarte gespeichert, wenngleich eine (verschlüsselte) Speicherung im Dateisystem des mobilen Computers gleichfalls möglich ist.

Alternativ wird ein mobiler Computer verwendet, der die sichere Identifizierung vermittelt. Der mobile Computer verwendet zwei Datenschnittstellen, eine für Nah- und eine für Fernverbindungen. Für die Nahverbindungen kommen die oben bereits erwähnten Einrichtungen in Betracht, über die bei den anderen Varianten der Personalisierer temporär angeschlossen wird. Für die Fernverbindungen kommen entweder Mobilfunkverbindungen oder andere Netzwerkverbindungen in Frage. Ein Routing dieser Verbindungen über die Nahverbindung ist ebenfalls möglich. Der mobile Computer kann daher auch ein Mobiltelefon sein.

Eine Variante dieser vermittelten Identifizierung erzeugt eine Zufallszahl im mobilen Computer und sendet sie einerseits über die Nahverbindung an den Sicherheitsmodul, der sie sogleich an den Personalisierer weiterleitet. Parallel dazu wird die Zufallszahl über die Fernverbindung direkt an den Personalisierer gesendet. Im Falle eines Mobiltelefons wird die vom Netzbetreiber mitgeteilte Anrufernummer ausreichen, um die Identität des Mobiltelefons ausreichend sicherzustellen. Im Falle eines generellen mobilen Computers wird bevorzugt eine gesicherte HTTP-Verbindung mit dem TLS-Protokoll verwendet, wobei auch eine Chipkarte zur Sicherung der verwendeten Zertifikate dienen kann.

Dabei kann die identifizierende Zufallszahl von jedem der drei Geräte erzeugt werden. Bevorzugt wird die Zufallszahl im Personalisierer erzeugt, der sie an den Sicherheitsmodul sendet, der sie an den mobilen Computer sendet, der sie an den Personalisierer zurücksendet. Erst dann wird die Personalisierung fortgesetzt. Die Zufallszahl hat hier dieselbe Funktion wie zuvor die Transaktionsnummer; sie wird lediglich erst bei Bedarf gebildet. Durch die Bildung im Personalisierer wird die Qualität gesichert. Entsprechend kann die Zufallszahl auch im Sicherheitsmodul gebildet werden.

Auch hier wird ein mobiles Gerät temporär an den Sicherheitsmodul angeschlossen und sichert die Identität des zu personalisierenden Sicherheitsmoduls gegenüber dem Personalisierer.

In allen diesen Varianten wird der Sicherheitsmodul dadurch personalisiert, dass der öffentlichen Schlüssel eines im Sicherheitsmodul erzeugten Schlüsselpaares von einem Zertifizierer zertifiziert wird. Das so erhaltene Zertifikat wird im Sicherheitsmodul gespeichert und ist für den nachfolgenden Betriebszustand kennzeichnend. Die Authentisierung gegenüber dem Zertifizierungsserver beruht auf einer temporären Datenverbindung zwischen dem

Sicherheitsmodul und einer von einem Bediener dazu benutzten mobilen Eingabeeinheit.

Patentansprüche

1. Verfahren zum Betrieb eines Sicherheitsmoduls, mit den Merkmalen:

- Der Sicherheitsmodul umfasst einen sicheren Schlüsselspeicher und mindestens eine Datenschnittstelle.
- In einem Personalisierungszustand wird eine Verbindung zu einem Personalisierer mittels der Datenschnittstelle hergestellt.
- In dem Sicherheitsmodul wird ein Modulschlüsselpaar neu erstellt und im Schlüsselspeicher abgelegt.
- Der öffentliche Modulschlüssel wird über die Verbindung an den Personalisierer gesendet.
- Von dem Personalisierer wird ein Zertifikat über den öffentlichen Modulschlüssel durch Signierung mit einem Signierschlüssel des Personalisierers erzeugt, an den Sicherheitsmodul gesendet und dort sicher abgelegt.
- Daraufhin wird die Verbindung abgebaut; der Sicherheitsmodul wechselt von dem Personalisierungszustand in den Betriebszustand.
- In dem Betriebszustand wird eine kryptographisch gesicherte Verbindung zu einem Zentralsystem aufgebaut, bei der der private Modulschlüssel benutzt wird und der öffentliche Modulschlüssel samt Zertifikat an das Zentralsystem übertragen und dort das Zertifikat geprüft wird.

2. Verfahren nach Anspruch 1, wobei ein erneuter Übergang in den Personalisierungszustand den Modulschlüssel löscht.

3. Verfahren nach Anspruch 1 oder 2, wobei im Personalisierungszustand die Verbindung zwischen Sicherheitsmodul und Personalisierer kryptographisch auf

Authentizität geprüft und gegen Verfälschung gesichert wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei zusammen mit dem Modul-Zertifikat ein öffentlicher Schlüssel des Zentralsystems übertragen wird, welcher im Betriebszustand für die Prüfung der Authentizität des Zentralsystems verwendet wird.

5. Verfahren nach Anspruch 4, wobei der öffentliche Schlüssel des Zentralsystems mit dem Signierschlüssel des Personalisierers signiert, das so erhaltene Zertifikat mit übertragen und von dem Sicherheitsmodul geprüft wird.

6. Verfahren nach Anspruch 5, wobei der öffentliche Signierschlüssel des Signierers von dem Zentralsystem signiert, dieses Zertifikat mit übertragen und von dem Sicherheitsmodul geprüft wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, wobei

- in dem Schlüsselspeicher des Sicherheitsmoduls ein öffentlicher Prüfschlüssel des Herstellers abgelegt ist,
- der Personalisierer seinen öffentlichen Signierschlüssel zusammen mit einem Zertifikat, gebildet mit dem Prüfschlüssel des Herstellers, überträgt,
- und der Sicherheitsmodul zunächst das Zertifikat des öffentlichen Signierschlüssel mit dem öffentlichen Prüfschlüssel und sodann die mit dem öffentlichen Signierschlüssel erzeugten Zertifikate prüft,
- und nur bei erfolgreichen Prüfungen in den Betriebszustand wechselt.

8. Verfahren nach einem der Ansprüche 1 bis 7, wobei in dem Sicherheitsmodul einmalig ein permanenter Identitäts-

schlüssel gebildet wird, der zugehörige öffentliche Schlüssel mit dem Prüfschlüssel des Herstellers signiert wird und das entsprechende Zertifikat im Sicherheitsmodul abgelegt wird. Der Identitätsschlüssel mit Zertifikat wird zur Sicherung der Authentizität gegenüber dem Personalisierer nach einem Challenge-Response-Verfahren benutzt.

9. Verfahren nach einem der Ansprüche 1 bis 8, wobei der Sicherheitsmodul an den Personalisiermodul einen Zeitstempel oder Zufallswert übermittelt, der bei der Bildung der Zertifikate in die Signatur mit einfließt.

10. Verfahren nach einem der Ansprüche 1 bis 9, wobei das Personalisiersystem einen Variationswert an den Sicherheitsmodul übermittelt, der bei der Erzeugung des neuen Modulschlüssels verwendet wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, wobei die mit dem privaten Modulschlüssel aufgebaute Verbindung mit dem Zentralsystem dazu benutzt wird, einen symmetrischen Schlüssel für nachfolgende Transaktionsverbindungen auszutauschen und im sicheren Schlüsselspeicher des Sicherheitsmoduls abzulegen.

12. Verfahren nach einem der Ansprüche 1 bis 11, wobei ein mobiler Personalisierer verwendet wird, der mit dem Sicherheitsmodul direkt über eine durch einen Bediener gesteuerte Verbindung verbunden wird.

13. Verfahren nach einem der Ansprüche 1 bis 12, wobei durch einen Bediener eine Einmal-Transaktionsnummer in den Sicherheitsmodul eingegeben wird, entweder direkt durch ein fest mit dem Sicherheitsmodul oder unmittelbar und direkt durch eine vom Bediener mit dem Sicherheitsmodul verbundene Eingabeeinheit, und die

Verbindung mit dem Personalisierer durch die Übertragung der Transaktionsnummer gesichert wird.

14. Verfahren nach einem der vorigen Ansprüche, wobei ein mobiles Gerät über eine von einem Benutzer direkt kontrollierte Nahverbindung mit dem Sicherheitsmodul und eine Fernverbindung mit dem Personalisierer verbunden ist, sich das mobile Gerät gegenüber dem Personalisierer identifiziert und dadurch das Sicherheitsmodul gegenüber dem Personalisierer indirekt identifiziert wird.

15. Verfahren nach Anspruch 14, wobei die Nah- und Fernverbindung lediglich zum sicheren Aufbau einer sicheren direkten Netzwerkverbindung zwischen Sicherheitsmodul und Personalisierer dienen.

16. Verfahren zur Personalisierung eines Sicherheitsmoduls mit den Merkmalen:

- Der Sicherheitsmodul wird mit einem Personalisierer verbunden.
- Der Sicherheitsmodul wird von einem Bediener über eine von dem Bediener bestimmte Schnittstelle temporär mit einem Identifizierer verbunden.
- Der Identifizierer sendet einen vom Personalisierer prüfbaren Identifikationswert an den Sicherheitsmodul, der diesen an den Personalisierer weiterleitet.
- Der Personalisierer führt die Personalisierung durch, wenn die Prüfung des Identitätswerts positiv ist.

17. Verfahren nach dem Anspruch 16, wobei der Identifikationswert eine vorab erzeugte Einmal-Transaktionsnummer ist.

18. Verfahren nach dem Anspruch 17, wobei der Identifikationswert durch eine kryptographisch

authentisierte Datenverbindung zwischen Identifizierer und Personalisierer ausgetauscht wird.

19. Sicherheitsmodul, enthaltend einen gesicherten Schlüsselspeicher, einen programmierbaren Prozessor und mindestens eine Datenschnittstelle, wobei durch die Programmierung des Prozessors sich der Sicherheitsmodul entsprechend einem der Ansprüche 1 bis 15 verhält.

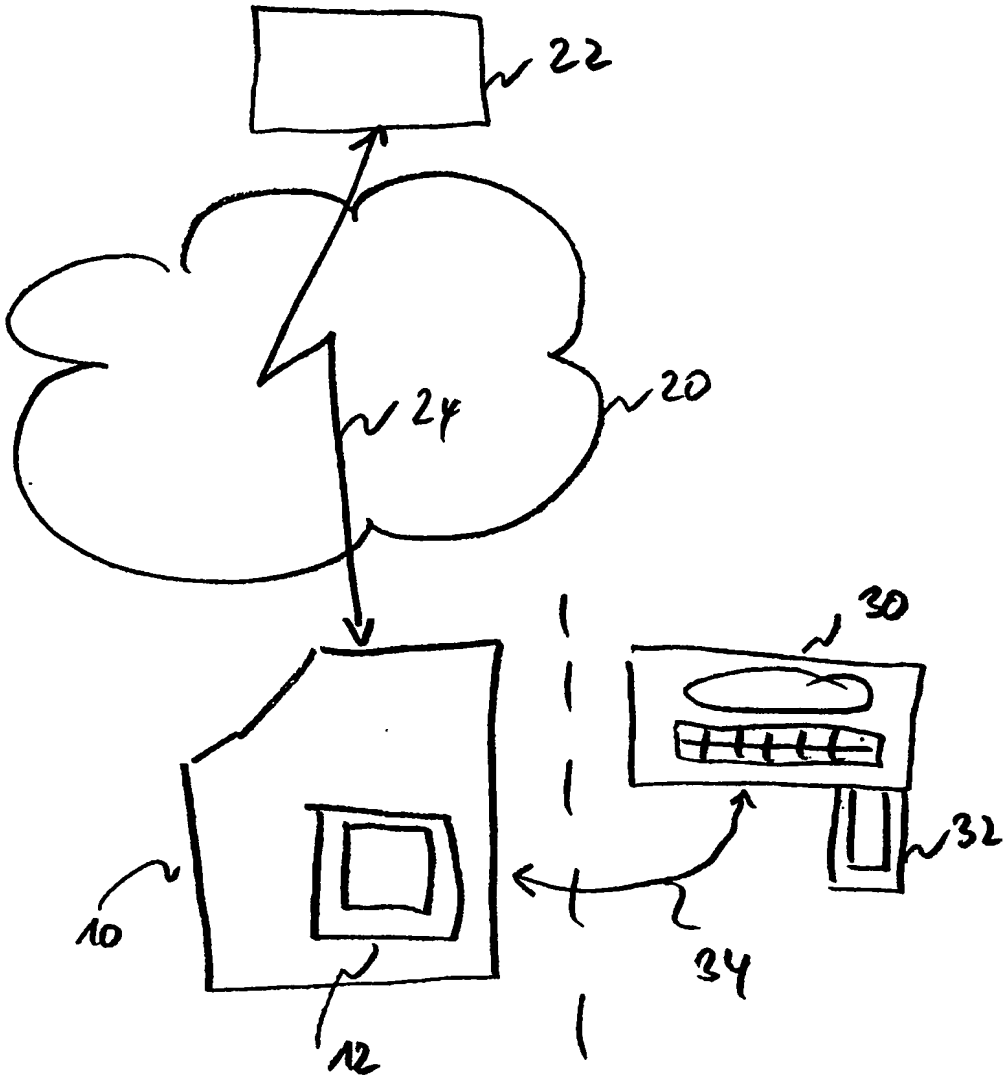
20. Personalisierer, enthaltend einen gesicherten Schlüsselspeicher, einen programmierbaren Prozessor und mindestens eine Datenschnittstelle, wobei durch die Programmierung des Prozessors sich der Personalisierer entsprechend einem der Ansprüche 1 bis 15 verhält.

21. Zentralsystem, enthaltend einen gesicherten Schlüsselspeicher und mindestens eine Datenschnittstelle, wobei durch die Programmierung des Zentralsystems sich das Zentralsystem entsprechend einem der Ansprüche 1 bis 15 verhält.

Zusammenfassung

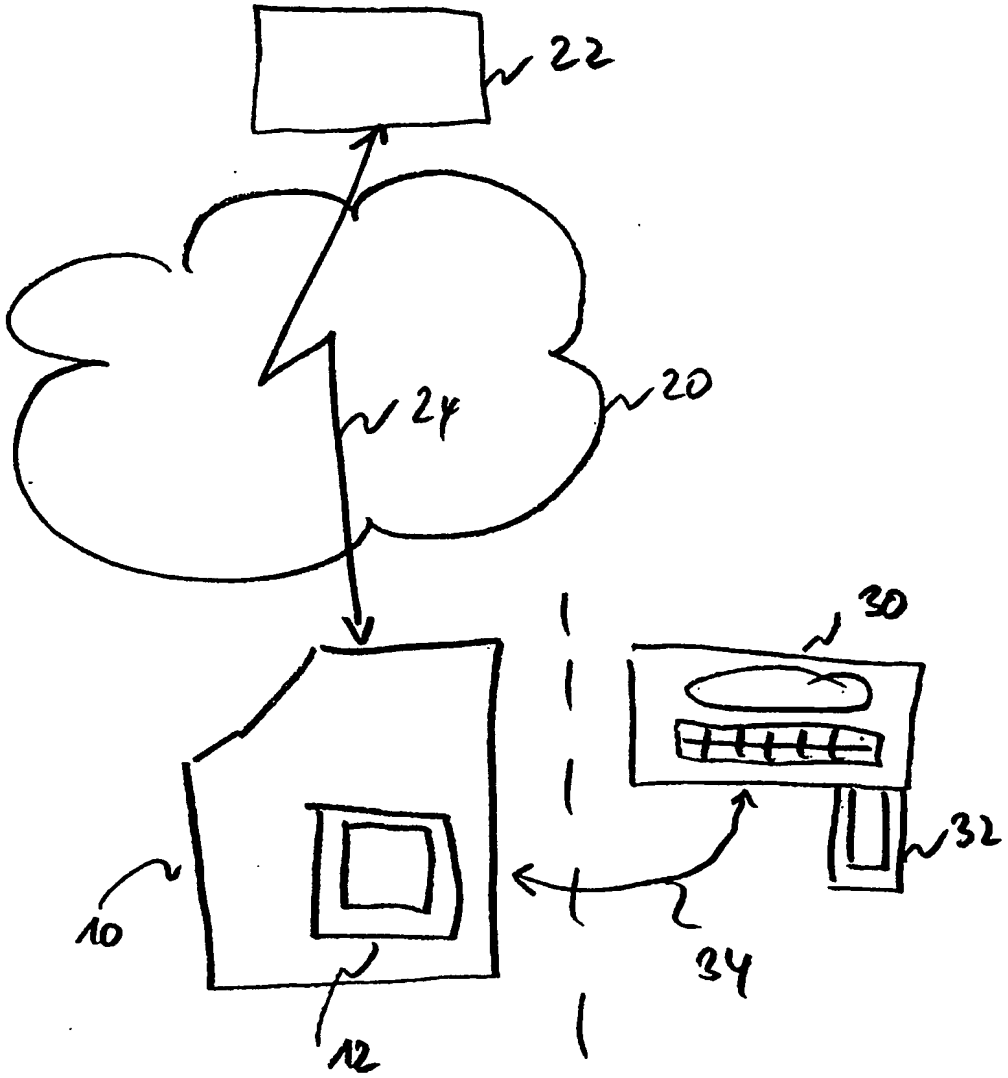
Sicherheitsmodul, Personalisierer und Verfahren zu deren Benutzung, wobei der Sicherheitsmodul einen geheimen Schlüssel eines Schlüsselpaares für asymmetrische Verschlüsslung enthält, der Personalisierer ein Zertifikat über den öffentlichen Schlüssel des Schlüsselpaares erzeugt und zusammen mit dem öffentlichen Schlüssel eines Zentralsystems an den Sicherheitsmodul sendet. Der Sicherheitsmodul verwendet dieses Zertifikat und den öffentlichen Schlüssel zur Sicherung der Kommunikation mit einem Zentralsystem, insbesondere im Bankenbereich.

Fig. 1



Figur 1

Zusammenfassung



Figur 1